Authorized Access for Information Derived from CLETS/NCIC

February 6, 2019

- **CLETS Policies, Practices & Procedures Sections**
  - **1.6.4 Confidentiality of Information from the CLETS:**
    - 1st paragraph: *Any information from the CLETS is confidential and for official use only. Access is defined as the ability to hear or view any information provided through the CLETS.*
    - 1.6.4.A: *Information from the CLETS is on a "right-to-know" and "need-to-know" basis.*
    - 1.6.4.C: *Accessing and/or releasing information from the CLETS for non-law enforcement purposes is prohibited, unless otherwise mandated, and is subject to administrative action and/or criminal prosecution.*
  - **10.1 System Misuse**
    - *A. Violation of the PPP shall be investigated by the agency head or his/her designee and reported to the CA DOJ.*

      Misuse is defined as CLETS information that is obtained or provided outside the course of official business; a "right to know" and the "need to know" must be established. The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions." Other than blatant misuse, the following are examples of prohibited/unauthorized use of CLETS by federal, state or local law enforcement agencies that include, but are not limited to:

      - *Providing information from the CLETS to another officer, individual, agency or company for unauthorized purposes*

- **FBI CJIS Security Policies Sections**
  - **4.2.3.1 For Official Purposes**
    - *…Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.*
  - **4.2.5.1 Penalties**
    - Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.
  - **5.5.1 Account Management**
    - *The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.*
    - *Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based*

on: 1. Valid need-to-know/need-to-share that is determined by assigned official duties. 2. Satisfaction of all personnel security criteria.

- **5.5.2.1 Least Privilege**
  - *The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.*
- **5.5.2.3 Access Control Criteria**

  Agencies shall control access to CJI based on one or more of the following:
  - *1. Job assignment or function (i.e., the role) of the user seeking access.*
- **5.10.1 Information Flow Enforcement**
  - *…Controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are: 1) Prevent CJI from being transmitted unencrypted across the public network, 2) Block outside traffic that claims to be from within the agency, 3) Do not pass any web requests to the public network that are not from the internal web proxy.*